FEDERAL TRADE COMMISSION

Do Not E-Mail Registry

Meeting

Tuesday, March 9, 2004

1:00 p.m.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

PARTICIPANTS:

From the Commission:

Michelle Chua

Colleen Robbins

Dan Salsburg

Louis Silversin

Afternoon Session:

Jerry Cerasale

Ronald Plesser

Joseph Rubin

Mark Uncapher

P R O C E E D I N G S

- - - - -

MS. ROBBINS: Today is Tuesday, March 9, 2004, and it is approximately 1:00 p.m., Eastern Standard Time. We are meeting today to discuss a possible National Do Not E-Mail Registry. My name is Colleen Robbins, I am an attorney with the Federal Trade Commission's Division of Marketing Practices. I am here with my colleague, Dan Salsburg, who is also an attorney in the same division. If you could all please just identify yourselves and your affiliations?

MR. CERASALE: I'm Jerry Cerasale, I'm with the Direct Marketing Association.

MR. RUBIN: Joseph Rubin, Executive Director, Technology and E-Commerce, U.S. Chamber of Commerce.

MR. UNCAPHER: Mark Uncapher, Senior Vice President and Counsel, The Information Technology Association of America.

MR. PLESSER: Ron Plesser, we represent several clients, ISPs.

MS. ROBBINS: As you know, under Section 9 of the CAN-SPAM Act, Congress has asked us to submit a report by June 16, 2004 outlining a plan and timetable for a National Do Not E-Mail Registry. Within that report we need to outline any technical, practical, privacy, security, or enforceability concerns the Commission has with such a

Registry.

To do this report, we are trying to get as much information as possible in a very short amount of time from many different sources. To help us facilitate in writing this report, any statements that are made during this session may be cited in that report, and that's why we have the court reporter here.

We thought that it would be best to structure this discussion by throwing out several possible Do Not E-Mail Registry models. We'll take each one in turn and talk about different concerns that you may have with each one regarding those several issues that I discussed: technical, privacy, security and enforceability.

One possible model that a National Do Not E-Mail Registry could take is based on the Do Not Call model, where consumers would register their e-mail addresses on a central database. Marketers would then receive a copy of that List and scrub their own lists, and then only send to those consumers who wish to receive e-mails. Do any of you have any thoughts on that type of model?

MR. RUBIN: If I could just start, this was a letter that U.S. Chamber of Commerce, Direct Marketing Association (DMA) among others, we all sent to Senator Schumer early on regarding the Do Not E-Mail Registry and some of the very serious concerns that all of us

had regarding such a proposal from a very early vantage point.

And those concerns persist, I think, among all four of the proposals that the FTC has cited. These concerns still present very serious hurdles to a Do Not E-Mail Registry. Let me go into some more specifics.

Enforceability has been one area, from the Chamber's perspective, from a business perspective, that will plague a Do Not E-mail List. We think that it is important to avoid putting additional burdens on businesses, on legitimate companies, companies that use e-mail legitimately, that follow the rules that spammers will not follow. For example, most companies who do business online post a privacy policy, voluntarily post a privacy policy, even though doing so enables the FTC to enforce it if they violate it. We don't want to put additional burdens on companies that follow the law, particularly vis a vis companies who clearly don't.

And we see the vast majority of spammers just don't follow the law now, and wouldn't use a Registry. And we think that hurdle, in and of itself, creates a huge burden due to a Do Not E-Mail List.

MR. SALSBURG: Would they not use a Registry because they couldn't be caught?

MR. RUBIN: I mean, that's the assumption -- they don't include their mailing address now as required by CAN-

SPAM, they don't include any markings, and they use false header information, all the stuff that the CAN-SPAM Act precludes now. So we have to assume that they would continue to violate any sort of law, any sort of registration.

MR. PLESSER: Could I make just one procedural point? It might be helpful if you could just tell all of the questions. Then we can go back to the first one. I think that some of these comments may cover the other two. We can be a little bit more efficient.

MS. ROBBINS: That's fine.

MR. PLESSER: But so we're all on the same page, that might be helpful.

MS. ROBBINS: Right.

MR. PLESSER: Then let's go back to talking about one.

MS. ROBBINS: Okay. We were going to propose four possible models for discussion. The first is based on the Do Not Call model, the second would be a domain wide opt-out model, where rather than having consumers register their individual e-mail addresses, domains would register their domain names.

MR. PLESSER: That that wouldn't be both, it would just be domain?

MS. ROBBINS: Of course we're not wed to any one of these, and we want to hear ideas about how they could

either work together, or be interchangeable in some way. These are just some possible ideas that we have heard, that we want to share, and are hoping to get your thoughts on.

The third would consist of a third-party forwarding service where similar to a Do Not Call model, consumers would register their e-mail addresses. That list would be held by a third-party forwarding service. Marketers would then forward their mail to the service -- not necessarily one service, it could be several, but all registered by either the FTC or some other agency to verify that they are authenticated forwarding services.

The e-mail marketer would then forward their mail to that service, the service would scrub the list and forward the mail. In effect the e-mail marketer would never see the scrubbed list, so they would not know who the mail is actually forwarded to.

The last possible model that we would like to discuss is an authenticated sender model, where consumers are actually not in the picture at all. Senders of e-mails would register with -- say the FTC. They would register their IP addresses and their domain names. They would then receive a registration number.

That registration number would somehow be embedded in every e-mail that they sent out, whether it be in the header, or encrypted somewhere. Then the ISPs would have

access to this registration list and be able to verify that an e-mail is actually from the sender who is supposedly sending the e-mail. The ISP could look at the mail and see the registration number and match that registration number with the IP address that the mail is actually coming from, to make sure that it coincides.

So those are basically the four models that we were hoping to discuss. And of course, we're willing to discuss anything that you may have thought of, any other ideas that you may have.

MR. RUBIN: Okay. Well, to get back to my earlier point, then, at least on the first three models specifically, the concerns about enforceability, I think, are paramount.

MR. UNCAPHER: And I think the reverse is true. We focused, obviously, on the burden issue of, you know, sort of good actors versus the bad actors. But the other side of that, of course, is the consumer expectation that if you sign up for a list or a process, whatever it would be, whichever of these four, they would, in fact, work.

And if -- this goes to your enforceability question -- if we set up something that doesn't either block out e-mail, but could be -- also we have the false negative issue -- keeps them from getting mail that they might otherwise want, and the workability issue, that there is a consumer expectation which is not being met.

MR. CERASALE: Yes, it's very much not like the Do Not Call Registry in the sense that whether I like it or not, the Do Not Call Registry works. Consumers put their names on the list and expect it to work. And it has worked.

I mean, there are complaints and things, and there are some glitches here and there that happen -- whether they really went through and actually signed up, and there have been some problems that way -- but basically, it works. The FTC made that -- gave a report out just recently on the overwhelming compliance.

The problem we see with an e-mail -- Do Not E-Mail Registry is that it won't -- right now, currently, it won't work because the number of people sending out e-mails that try and hide who they are, actually -- they violated the law before the CAN-SPAM Act. They were deceptive in their own right. So I think any state or through Section 5, you could go after them, and it's difficult to find them.

And so I think that it wouldn't work -- our view is that it wouldn't work in the beginning, and it becomes -- and from a marketer's standpoint, it gives us even a worse name. The marketers who are legitimate would be following the law, not sending out those e-mails, but look at these guys, these marketers, they haven't stopped it, they're sleazy, all of them are awful, and they get painted with a broad brush as the bad guys.

So, it also is not just consumer expectation, it becomes a negative towards the industry, whereas for example the Do Not Telephone List has not become that negative towards the industry.

I mean, there are -- nothing is perfect, but it hasn't. You haven't been hit with a broad brush that marketers are awful. They are honoring the list, which is actually, from that point at least, builds up the honest marketer. But this would tear down the honest marketer.

MR. PLESSER: I think there is a couple of beginning points that need to be made. I brought a copy of something published by the AARP on whether or not we need a new law, and I brought a copy for you guys to have that.

MR. SALSBURG: This is just for the court reporter's reference -- what he's referring to is something in the AARP bulletin dated February 2004 on page 14.

MR. PLESSER: Right.

MR. SALSBURG: Under "Face Off: Do We Need a Stronger Federal Law to Curb Junk E-Mail?"

MR. PLESSER: And my first sentence is, "Yikes."

MR. SALSBURG: I don't see a "Yikes" in here.

(Laughter.)

(Several people speak simultaneously.)

MR. PLESSER: Let the record reflect that there was laughter.

(Laughter.)

MR. PLESSER: The -- I guess one of the points in that article is during Christmas time this year, $18.5 billion worth of commerce was done on the Internet, whether web sites, e-mails, electronic commerce.

So, I think we have to look at the problem in this wider scope. We all want to stop spam, we've all done a lot to support legislation to stop spam.

But I think a Do Not E-Mail Registry, or at least the first three of the options that you suggest, in our view, would jeopardize that level of commerce, which also relates to jobs, if somebody makes an inquiry of the web site is it consent, is it not.

Your provisions -- and I'm not sure at this point of any more specificity -- but there is no indication that there would be an EBR, they be a consent way around being on the list, what EBR – existing business relationship -- we're not asking for those things here.

I think all of us oppose a List, but to judge the effectiveness of it, you know, from what we see here, is really incomplete, in terms of trying to understand really how such a thing would work. I think all of the instincts of my colleagues are things that I would agree with on a privacy approach.

Clearly, if you submit a list to the government, if

that's the way it would work, and they would knock out the people on the list, there is a real danger that the person who solicits the list can just do a very simple application, and find out who is on the Do Not Call List. There is a real danger, particularly with some of the bad actors.

Someone in the Commission said that 90 percent of the people doing telemarketing are legitimate, and 90 percent of the people doing unsolicited commercial e-mail are probably not legitimate.

So I think that those are really concerns that we have, that the privacy and security of the system, of having a system of opt-outs would be very, very difficult to enforce, in terms of the individual.

The FTC is in somewhat a different area, but where the FTC looked at how many people had ADV in the header in the study you did last year. And it was a California requirement. And you showed only two percent compliance with that. The same case would be seen by bad spammers here, would be low, the compliance would be low, the privacy danger would be high. Your authentication issues we have even seen with Do Not Call Registry would be even more weighing in this environment.

And then finally, you know, it will not be easy to locate the people who don't use the List? If people are using the List, they have to be rewarded by finding the

people who aren't going to use the list. There it has to be some commercial parity.

It's extremely difficult to find the bad guys, whether or not there are a lot of them or a few of them, it's hard to find them. And then, if you stop them, they come up in another direction.

So, I think generally, the sense is that a Do Not E-Mail List won't work, and it's dangerous.

MR. CERASALE: One of the things that I'm trying to find -- I mean, our view is that we have created the CAN-SPAM Act, and you have some provisions where you don't have to prove fraud any more, it's just you have a valid postal address you have them, and the key is to try and find them, which is the key for any kind of enforcement on any of this stuff.

Any of these four elements would be trying to find -- well, maybe the fourth one might not be, but -- as much -- but your first three is trying to find them, and that's going to be a real key here for anything.

And I guess from our point of view about time, let's give a little bit of time to go after people under CAN-SPAM, to see if that can work. I mean, right now, the way CAN-SPAM works you have the legitimate guys -- and we know that, through all of the stuff that we have done with seminars trying to say what it is, and because the law went

into effect before you had even an opportunity to flesh out the regulations, which will come about.

But eventually, we're going to get some enforcement of those not following and hopefully we will see what that effect has.

And so, I think, from the point of view where DMA is, at least even on timing, is let's take a look and see what we have right now, because the enforcement problem that CAN-SPAM has is the exact same problem that this List has.

MR. PLESSER: I would think government resources to impact CAN-SPAM -- you know, to enforce CAN-SPAM, with the FTC and Department of Justice would be a much higher priority to get that law up and going and enforced. And there is great industry support for enforcement of that statute.

MR. RUBIN: I'm sorry, one point we should have made from the beginning is all of us around the table --

(Several people speak simultaneously.)

MR. RUBIN: One point we should have made from the beginning, and emphasized from the beginning, is that we all support stopping spam -- spam has become much more than a nuisance.

The Chamber testified before the Judiciary Committee in favor of an earlier version of the CAN-SPAM Act. Studies have shown that it's costing employers $10 billion or more for their employees to, you know, waste their time going

through -- combing through their e-mail boxes and losing vital e-mails or time. And on the other side, consumers are deleting the legitimate e-mail along with the junk.

So, from that perspective, we -- and I think all of us -- endorse the CAN-SPAM Act. We very strongly believe that there should be a federal, uniform federal standard to enforce -- to go after the bad spammers. I mean, our companies don't use false headers, they don't do any of the stuff that the CAN-SPAM Act is aimed at, is focused at. So --

MR. CERASALE: Yes, if we violate CAN-SPAM, you will be able to find us.

MR. RUBIN: Yes, if you are a legitimate company, you will be able to find us and find our members. And you know, to echo I guess Jerry's point, we want to give the CAN-SPAM Act a chance to work, give you guys a chance to take advantage of the tools that CAN-SPAM has implemented.

So, for example, we came out very strongly in favor of the McCain amendment. You know, it's not usual that the Chamber of Commerce would support some even modest additional burdens on businesses, but in the instance of the McCain amendment, we have said marketers who are going to use e-mail should have -- should do some research into the people who are doing their e-mail marketing to determine whether or not they are doing anything illegal or suspect.

So, you know, we think those types of tools really

give you -- give the FTC -- a strong leg up, in terms of maybe not finding these spammers themselves, but finding those that hire the spammers.

MR. PLESSER: And there is a great development ongoing of technological developments, and I think a lot of that was encouraged by the FTC workshop in June. I know since that time, the Postini Company has rolled out one of the programs that actually was discussed there, and it works quite well.

Technology alone isn't going to solve the problem, but technology is starting to solve the problem. You know, 10 years ago I was probably -- or maybe less; I guess 7 or 8 years ago -- I was in the same room talking about cookies, about how that was going to invade privacy and should there be legislation. And you know, with the FTC dialogue, with the industry, it got worked out, and you know, cookies just aren't the kind of the threat that they could have been or were.

The same is here with spam, that we have legislation, we do have tactical -- everyone in the trade associations or associations sitting at the table worked very hard on creating technical alternatives. There are services out there now that can help manage spam effectively for end users.

It still remains a significant problem for ISPs,

but I think the ISPs don't see any particular relief on Do Not E-Mail Lists.

MR. SALSBURG: Let me just ask a question. A number of advocates of a Registry have said that even if illegitimate marketers who would not comply with the Registry comprise 90 percent of unsolicited commercial e-mail, there is the other 10 percent that would comply. And there would be a net benefit, then, in the reduction of 10 percent of spam. Any thoughts on that kind of --

MR. CERASALE: Well, there clearly would -- you would get a drop in e-mails. I don't know how significant of a drop. I mean, I guess if you assumed that every e-mail address in the country went on the list, you would get a 10 percent drop in the amount of e-mails coming out.

What does that -- what's -- you have to take a look at what's the cost of that. You would take that $18 million of last holiday season, and it would be gone.

MR. PLESSER: Billion.

MR. CERASALE: $18 billion, excuse me.

MR. SALSBURG: Was the $18 billion a result of unsolicited commercial e-mail, or was it a result of --

MR. PLESSER: No. I'm trying to be very clear, that it was $18.5 e-commerce. But part of how e-commerce works is they communicate with customers. It's unclear that any of these are here, whether or not customers would be

treated differently than not, so I think everybody's working assumption is that if you are a customer, if you are on the list, you could be e-mailed to.

I just bought a set of pots from the Internet. Can they write me an e-mail back and tell me when a companion set is available, or something like that? It's part of the commerce.

MR. UNCAPHER: Right. And one of the costs Joe alluded to, the concerns the industry has, but one of the costs of e-mail is clearly that mail with -- that the consumer has a relationship with doesn't get through or gets lost in the inbox.

And one of the concerns about some of the proposals is that you end up with a false positive screening process, that consumers would want, where clearly there is a relationship, or whatever, doesn't get through.

So, the benefits, the savings to consumers who may have registered to get updates and what have you, end up getting lost because of either the screening mechanism or the caution on the part of organizations, entities that would be communicated with them.

MR. SALSBURG: Maybe you could explain why a Registry would increase the false positive rates?

MR. UNCAPHER: Well, the concern would be that with -- going back to Jerry's example, that the reluctance that

consumers who -- people who would want to communicate with consumers would be less likely to use e-mail for fear of running afoul of the registration.

And the nature of the registration, since it's kind of very broad, broad based, includes all e-mail. I signed up for the registration even though there are maybe -- as a consumer -- categories of e-mail that I would want to receive. I would want to continue to get certain kinds of updates.

The registration doesn't have the ability to be able to effectively discern, you know, where there was a relationship, where there isn't a relationship, where there may be some combination there. So, a marketer, or somebody trying to communicate with me -- American Airlines, let's say -- would be less likely to want to send the statement.

MR. SALSBURG: So you chill --

MR. UNCAPHER: It would chill the legitimate --

MR. PLESSER: And it's not entirely clear to me how the ISP, you know, would know. So if you get on the list that you don't want to receive e-mail, it's very difficult for the ISPs to know who wants mail and who does not. If I'm a frequent flyer with United, how can they distinguish that -- assuming a whitelist -- how can they distinguish that between, you know, somebody sending Viagra messages out?

I think ISPs operate at a level that they really can't go into the content on messages and make that kind of routing and sorting. So I just think we see a real mess in it, because at least as the proposal that's out there -- cut off wanted mail, as well as unwanted mail.

PARTICIPANT: Yes.

MR. PLESSER: It would be very difficult, at least as we understand it, to be able to do that.

MR. RUBIN: Well, just as an example in increasing the false positives, two of the proposals, the domain wide opt-out and the third-party forwarding service, would have adverse effects, for example, if I'm a customer of -- if I said, you know, "Send me special offers," if it's filtered through a third-party service, it could get filtered out, and then -- the customer wouldn't receive the e-mail, even if perhaps they specifically opted-in to receive additional pieces.

So, there really is a danger of dramatically increasing the amount of false positives that --

MR. SALSBURG: I guess I'm not following that.

PARTICIPANT: Which is a double back to, I think, the point -- the question you raised at sort of the outset of this particular exchange, was the sort of relaying that the advocates come and, "Well, maybe we can't get the 90 percent,

but we can at least focus on some of that 10 percent with legitimate people."

Well, our contention would be that within that particular subset, there are a fair number of -- there is a fair amount of communications that consumers would want to receive. It's not to say that they don't have very real -- as we all do -- objections to the 90 percent that you can't get a hold of. The problem is you really can't do a discerning analysis among that 10 percent that we talked about. It would be subject to different interpretations that --

MR. SILVERSIN: May I ask a clarifying question?

PARTICIPANT: Sure.

MS. ROBBINS: I think just for the record -- I don't think we put your name on the record.

MR. SILVERSIN: My name is Lou Silversin, S-i-l-v-e-r-s-i-n. I'm an Economist.

MS. ROBBINS: With the --

MR. SILVERSIN: With the Federal Trade Commission.

When you speak, Joe, of this third-party service, I wonder if the following is what you have in mind. It would be a Do Not Spam Registry, but a consumer might have indicated that he wants to get certain e-mails. And then there would be a third-party service that would sort of try to reconcile which e-mail should go through and which should

not, and they would make errors. Is that your point?

MR. RUBIN: Well, they not only would make errors, they would perhaps purposely weed out e-mail that -- if I, unbeknownst to a third-party -- to the forwarding service, if I went to American Airlines' web site and registered for their, you know, weekend specials, or whatever it is, all of a sudden American Airlines starts sending me e-mail through the third-party service.

MR. SILVERSIN: Right, right.

MR. RUBIN: But I am on the Do Not E-Mail List. So the third-party service says, "No, sorry," bounce back, you don't get this.

MR. CERASALE: Well, it's not even a bounce back.

MR. RUBIN: Right, I mean --

MR. CERASALE: American Airlines would never know.

MR. SILVERSIN: I'm not arguing, I'm just trying to understand it, but wouldn't there be some mechanism by which when you had signed up to put yourself -- that you had opted-in to a particular e-mail from a particular company, that that message would go to the third-party service? Otherwise, what sense does it make?

MR. RUBIN: Well, I mean, that also goes back to the enforceability question. One of the main questions with all of these is enforceability. If I am a dishonest e-mailer anyway, why not just send --

MR. SILVERSIN: Oh, sure, sure. I understand all of that.

MR. RUBIN: Okay.

MR. SILVERSIN: I mean, we're taking that for granted, that it's not going to work on the 90 percent. I'm just --

MR. PLESSER: But one of the factors -- maybe this is not completely responsive -- we have found in the Do Not Call Registry that there were a lot of complaints that came through in the early period and later, where there was -- where people complained about calls where there were various reasons for why they got the call, either perhaps a franchise person who used the same name but wasn't really a related company.

There was a number of those situations, where consumers got upset. And there were other situations. We use -- in the system I use and have personal experience with, there are false positives all the time. They have a very nice way that you can look at it and weed out and kind of open it up for the ones that they stop, but I think that the experience is that it's -- if I go on the list and say, you know, "I want to be on the list," and then I don't get my frequent flyer stuff, I'm going to, you know, I'm going to be upset.

MR. CERASALE: And you're going to blame the

company.

MR. PLESSER: Who is going to enforce that? The company enforces it -- if it's really an issue of United Airlines, and you say United Airlines has the obligation not to mail to anybody on the List, that's one thing. If the ISPs are part of that obligation, then I think the ability, the danger of having false positives arises --

MR. SALSBURG: Or, as Joe was saying, the third-party forwarding service model also. Any time there is some party engaging in the filter other than the sender --

MR. PLESSER: The third-party registration model as a mandatory program really confused us, and I don't think we really understand -- I mean, we, DMA have what you would call a third-party service that's being managed, I think, internal.

But that's a voluntary program that members -- you can register and members or anybody else can get on it. And that works as a voluntary program. But if it's a mandatory program, how would they forward? How would you make sure? We're just not quite sure what the scope of it is, if it's mandatory.

If it's voluntary, then we can understand it. You know, United Airlines -- I belong to certain lists, you know, we honor people who opt-out, and so and so. But if you're going to opt-out to all of them, and there is, let's say, 100

of these or 50 of them, then the burden of having to coordinate all the lists, take care of the duplication just creates, it almost seems to us, a nightmare scenario that I'm not sure you had intended.

So, we're not quite sure how the private third party would live, would work mandatorily on the theory that if you were a marketer you would have to probably participate in each and every one of them. And if you did have to do that, then it's -- it would seem to me pretty out of control.

MR. SALSBURG: Let me describe the third-party model.

MR. RUBIN: I'm sorry, before we get into that, can I just go through a couple of more concerns about the advocates' position, just so we can close that loop out?

You know, we already have an opt-out in the CAN-SPAM Act, so customers already have the ability to --

PARTICIPANT: That 10 percent.

MR. RUBIN: Yes. If they don't want to receive e-mail, they can opt-out. Second, companies don't -- you know, the last thing companies want to do is upset their customers and potential customers. If I get too many e-mails from target.com, I'm not going to go there online, I'm certainly not going to shop there in person. No company wants to be caught in that box.

So, you know, companies -- retailers, marketers, whoever, legitimate companies -- are extremely careful about not overburdening consumers under current practice.

So, you know, we think that having a Do Not E-Mail List and giving companies the ability to say, "Well, we're not going to send continually to Joe because he's going to get upset," you know, I think the market already deals with a significant amount of that.

Additionally, there are -- you know, we didn't really get into these yet -- but security and privacy concerns about a Do Not E-Mail List generally that, you know, even if you stop the 10 percent, but if you dramatically increase security concerns or privacy concerns, you may end up taking two or three steps back, instead of a step forward to stop that 10 percent.

MR. PLESSER: I -- about the privacy, I thought we did talk about it before, but I'm happy to come back to that, but -

MR. SALSBURG: The forwarding model --

MR. CERASALE: Explain the third-party model.

MR. SALSBURG: Imagine the post office, but in an e-mail setting, with a marketer delivering your letters to the post office. The post office then has a copy of the master Do Not E-Mail Registry, and scrubs the list, and sends along only those that are to addresses not on the list.

Imagine this model only for unsolicited commercial e-mail. You pointed out a number of flaws if this model applied to transactional messages. That's the model.

MR. RUBIN: Is it a must-carry on the ISP side? Because obviously, that's a huge concern. They're not telecommunications carriers, they're not regulated by the FCC. So if it's a must-carry, that presents a significant amount of problems on their part.

MR. SALSBURG: Let's assume it's not a must-carry, that this is merely a method of effectuating a Do Not E-Mail Registry where marketers do not get copies of the database. It removes that security risk.

MR. PLESSER: So what you're saying is that a marketer would have to choose who it wanted to deal with, but it would have to deal with a third-party, who would then -- a trusted third party -- who would wash the list before it went out?

MR. SALSBURG: Exactly.

MR. PLESSER: But it would still be one central list that the government would put together?

MR. SALSBURG: Right.

MR. RUBIN: That goes back to the opt-in question, or whether or not it's the -- you know, the false positive question, whether or not someone opted-in, whether or not it's a transactional message or an unsolicited message.

You know, all those types of questions have to be --

MR. PLESSER: But I just think that it's irrelevant from that perspective, to solve at least the privacy problem and security problem, because if you know who -- if you give them the list and then you can find out who was taken out, and therefore you know who was on the Do Not Call List.

MS. ROBBINS: No, the e-mail marketers would never know who was not on the list. They would submit their e-mail, and it would get forwarded, but they would never know what didn't get forwarded.

MR. CERASALE: So, a marketer would send out 100,000 e-mails -- just a round number; I know it's small -- but 100,000 e-mails, and 50,000 of them get through, 50,000 don't. So, from my marketing standpoint, as a marketer, I'm going to get a response -- let's say get a response on my e-mail, or 1 percent, so I get about 500 back. I think that that's a half a percent response rate, because I have no idea, I can't measure who received or who didn't receive the list.

I mean, that takes marketing and stands it on its head. So, from that perspective, from a marketing perspective, you have just taken e-mail and no longer made it measurable. I can't measure. I can't determine whether or not --

MR. SILVERSIN: What if they could tell you how many were scrubbed without telling you the individuals who were removed?

MR. CERASALE: Well, I don't know -- I guess. The problem -- that could do some. The other thing is -- let's go from an efficiency standpoint. I'm constantly going to send out e-mails. I want to always give the same e-mails to increase -- the third-party forwarder is always going to have to constantly scrub names that I or -- that I would have known, if I got it back, and wouldn't have been on the list to scrub. So you dramatically increase --

MR. SILVERSIN: You won't know who has already seen it and who hasn't seen it?

MR. CERASALE: That's right, I wouldn't know that kind of thing as well, so it would mess up marketing. But also, just look at it from the point of view of running the list, if I -- even if I go to a Do Not Call List, I use a service bureau to do the stuff and do the scrubbing, they're going to tell me who is on a List, on the National Do Not Call List and so forth, and therefore, I don't, then, send back another time if I get another campaign that's going out by telephone, those phone numbers. Because I get charged by the number -- by the size of the list and how it gets scrubbed.

The reason I get charged that way is because that's

how costs run in running a list. The third-party forwarder, if I never know, is going to -- the costs of this are going to be very, very high because you're never going to get marketers sending you clean lists to scrub for just maybe add-ons. You're always going to have to start from scratch. So very -- from the beginning. So, it dramatically is going to increase the cost of --

PARTICIPANT: Of scrubbing.

MR. CERASALE: Of scrubbing, which is a cost to us.

PARTICIPANT: Well, the --

(Several people speak simultaneously.)

MR. SALSBURG: Conceivably there could be a third-party forwarding service that maintains a copy of the list that you submitted originally, a scrubbed version, and then just checks the additions? I mean, it just changes who is holding the scrubbed list.

MR. RUBIN: I would have to give the list -- I would have to go all the time before -- I mean, I guess there could be ways --

PARTICIPANT: That also makes it more difficult for targeted marketing, you know, to actually decrease the amount of e-mail traffic.

MR. RUBIN: Yes. You would actually have to, ironically, increase the amount of traffic to get -- you know, if you knew that a small percentage of your e-mails are

getting through, you would increase the size of your mailing. There would be no way to target, and the size of the mailing would ironically go up.

MR. PLESSER: And as you said, it's really aimed at the 10 percent only, and then your costs are going to probably double, going to significantly increase, because you have the government costs, they're going to charge a user fee as you would do in other circumstances, and then you're going to -- and then whoever the third-party mailer is is going to charge additional for that.

So, part of one of the issues that we haven't talked about is the -- the competitor issues of having a freer e-mail marketplace. Your proposal would double and triple the cost of people who legitimately want to go e-mail, and you know that you're not catching the 90 percent of people who would never sign up for these services or sending out bad e-mail to begin with.

MR. SALSBURG: And Joe, your point was that not knowing the response rate, the intent was then to send more?

MR. CERASALE: Yes, you can't plan as well. One of the problems with spam is that with other forms of marketing there at least is some incentive, economic incentive, to target. E-mail does not have such an economic burden, cost. To add another name on is virtually zero. I mean, it isn't, but it's -- for this conversation, it's close enough to zero,

so there is not an incentive to target.

Scrubbing, if you have to go through and scrub, and so forth, the incentive is to not incur those costs, and the idea to reduce spam is to try and get our members to try and target who needs it and who wants it. And it just becomes a part of a disincentive to do it.

There is one thing on a National Registry, as we look forward, and that would be both in one and three, the National Registry and the third-party forwarding. We haven't talked specifically on domain wide yet.

Unlike those two -- I don't know how much technical, but at least the cost, and how one has to use it and the burdeness of it -- the 57-plus or whatever million number Do Not Call Registry takes some time. Certain larger users are maybe more efficient in getting it, but others aren't, and you run through it.

One of the things that happens in the phone is that the government -- in a sense, through NeuStar -- controls phone numbers, and who gets them, and so forth, and there is a 16 percent churn rate -- at least we have heard; it may not -- 16 percent churn rate in residential phone numbers, and AT&T, your contract was -- is delisting numbers when people have moved.

So, if the List, over time, is going to grow, or each month you're going to have a significant number of drops

and you're going to have adds as well, as you go along, there is no such government issueness -- for want of a word -- no government issuing of e-mail addresses.

And we had heard -- and I don't know if it's true any longer, Mark, you may -- at one point we talked about churn rates of addresses, mail addresses the churn rate is 20 percent in the U.S., phones have been 16 percent. I mean, we had heard that the churn rate -- I don't know if the churn rate, but the life span, the life span of a phone number -- of a street address -- was 5 years, the life span of a phone number was 6 to 7, the life span of an e-mail address was 6 months.

Now, that may or may not be true any longer, it may be a little bit bigger than that ---

MR. UNCAPHER: Well, I think you touched on a point I wanted to talk about with domain names, just focusing on the different ways -- I hope this is responsive --

PARTICIPANT: Go ahead.

MR. UNCAPHER: But the different ways in which people receive e-mail service, and I think the domain name is probably a good way to sort of drill down on that.

You know, it's true, yes, one model is sort of -- the residential consumer has an AOL or other ISP account, but much of mail, as Joe referred to before, is also at the employer's -- on the employer's account.

So, the relationship with the ISP is entirely different. They would just be passing through the traffic, and in effect, the burden would be on the company's own network to be able to do screening. That's sort of another set, other than the consumer/residential model.

And then the consumer uses a third-party portal, like, say, Yahoo!, which is not an ISP, so to speak, but is a mailbox of convenience.

So, in each of these where you may be envisioning an ISP having a particular role, it's worthwhile to think about there are different circumstances in employer, residential, and third party that have sort of different kinds of characteristics and put different burdens.

So, for example, with the domain wide, while it's certainly entirely possible that anybody who wants to set up an account can set up kind of a blank account with -- you know, which unless through a kind of randomly -- an e-mailer, a spammer identifies that as a potential account, you could have that and it's certainly available in the marketplace.

The problem is probably that that's not an account which the consumer would use very often. Certainly the business account is one -- you know, "I get a lot of spam because my e-mail address is on my web site, but that's because I have to do business that way."

So that sort of unlisted number issue that --

really wouldn't be very useful for consumers who are out sharing e-mail addresses for completely legitimate reasons, or just because they happen to be out, and doesn't really kind of solve that set of issues.

Again, if somebody wanted to, they certainly could do it now. They could have kind of an unlisted account that they only give to their friends and family and in all probability, the percentage of spam that they get would be, you know, virtually nonexistent. But that's not, obviously, what ends up happening.

Now, you mention -- and I mean, to pick up where Jerry was is that there are -- as businesses change the routing information, as they change their ISP, as consumers change -- are moving from -- my wife is moving from Comcast to Starpower in two weeks, so she will have an e-mail address change. That's probably about every six months seems to be about the average that she has got.

So that is a very common phenomena, understanding these kind of changing relationships that people have with ISPs. Phone numbers are probably a lot more durable.

MR. CERASALE: Yes. And what that does is it raises the question of the -- if you did have a Registry and you're one or three, it becomes unwieldy. It takes a lot of time to run the Do Not Call Registry with the expense, and we have a cleaning process on it. And you don't have that

cleaning process in the Do Not E-Mail List.

I have a Yahoo! address, e-mail address, that I picked up six years ago. I don't think I have looked at it in five years. So I mean, it may be dead, it may not be dead, I don't really know, because as you move on and as we get bigger push to broadband, you're going to get a shift in -- a whole shift, nationwide -- in e-mail addresses, most likely.

And it's just an issue of how this is going to work, at least in the short run. As you look at quickly what's going to happen, we see that there doesn't seem to be a means to clean the list, so the list becomes very, very stale and very, very large. And you have -- you're going through a scrubbing process -- whoever is doing the scrubbing process, becomes much, much more expensive and much less efficient because you have e-mail addresses that have died.

You know, that's one of the things, getting to --

MR. UNCAPHER: Yahoo! has a practice, which is probably instructive, of dropping accounts after somebody hasn't accessed it for 90 days, something like that.

MR. CERASALE: But if I put my --

MR. UNCAPHER: But the interesting question would be whether or not -- and I just don't have the answer -- whether after some point that could become -- another

consumer could access that account, you know, and simply --

MR. CERASALE: Well, not even -- the point is -- JerryCerasale@yahoo.com, and I got it six years ago and I haven't looked at it in five years. If someone sent something to JerryCerasale@yahoo.com, it's gone, because Yahoo! has wiped it out. But I put JerryCerasale@yahoo.com on the Do Not E-Mail List. It stays forever, because it's on there.

MR. UNCAPHER: At some point, Jerry Jr. could sign that, and --

MR. CERASALE: That's true. Well, I put Jerry -- because of spam, I do Jerry Cerasale. People know my full name, and also dictionary attacks tend to not believe and not go out that far, so many letters at that point, I have found. But that's another issue.

But the point is, that's right, if I were Jerry1, and I was the first person at yahoo.com, and eventually they wipe it out and some other Jerry comes on, Jerry1@yahoo.com --

MR. SALSBURG: So there are two issues.

MR. CERASALE: That's another issue. I didn't realize that. Mark raised that one again --

MR. SALSBURG: Let me see if I can paraphrase them. The first is that the database is ever-expanding, unless you had a system set up like the phone company's, where there was

a method for essentially deactivating, or delisting inactive e-mail addresses.

And the second one is that the preference from one consumer may be inadvertently transferred to another who takes over the account, or signs up for an account that's expired and gets the same name.

PARTICIPANT: Right.

PARTICIPANT: That's true.

MR. UNCAPHER: Probably it's more common when you have a situation where people have registered, you know, Mark@ita.org, and I leave and a year from now there is another Mark, same e-mail address.

MR. PLESSER: We would all oppose the domain wide opt-out on the record -- but I think it would -- it really requires a very precise definition of what UCE is, because there is going to be a lot of mail.

You know, what if I find an e-mail address -- commercial, I guess -- but if it's a long lost friend, or a long lost client and I send stuff to him, it's not going to get through. What's the definition? How is it defined so that if I'm on a domain that blocks out all UCE, what's the false positive issues? Did I intend to have particular cut off?

I think it presupposes that we can walk around this table and come up with a very clear, precise definition of

UCE because clearly, if it's a domain wide block, we don't want it to be a domain wide block for all e-mail, or even all commercial e-mail. You've got to say, "Well, UCE," well, how do you define UCE?

The domain wide opt-out is an -- extremely dangerous, in terms of commerce. It could cut commerce off. I don't know that we have had extensive conversations at the ISPs, Mark might want to talk about that, but the whole idea of the Internet is to be able to communicate and to have a commerce available.

Now, you can choose, as you suggest, you know, you could choose to be in one that's opted out or one that's not opted out, but I don't -- the implications of that and the cut off of the ability to communicate would be most disastrous in that one.

MR. SALSBURG: Before you get there -- Ron, how would you differentiate between the domain wide opt-out system which was sender-policed versus a situation where the ISPs had somehow used their filters to effectuate the opt-out.

MR. PLESSER: What do you mean sender-policed, that the sending ISP wouldn't --

MR. SALSBURG: Or that you, as the marketer, you would scrub your list and anything that -- for instance, say AOL said, "No spam," you just wouldn't send to AOL.

MR. PLESSER: Well, they say that now. MCI says that now --

MR. SALSBURG: So then, how is that different?

MR. PLESSER: And they have whitelist programs that let you go on the system if you, you know -- very large quantities, as we know. So that system, to the extent that that's what you're looking for, that system is working. The whitelist system works very well.

To enforce it by statute -- and we will talk in the last option more about whitelists, and gold lists, but --

MR. SALSBURG: Let's do that now then.

MR. PLESSER: I think there is a big difference between voluntary and mandatory.

MR. SALSBURG: There are roughly 1,500 ISPs out there, and some of them are going to have different whitelist programs. From a marketer's standpoint, is a centralized domain opt-out list a good thing? Because then you would at least know who has the no spam policy without having to figure out all 1,500?

MR. PLESSER: It depends precisely on your definition of what spam and UCE is. And I don't think we have gotten there yet. We're close to getting there.

MR. UNCAPHER: And I want to underscore that, that the -- while there may be 1,500 ISPs, you have a variety of methods, mechanisms --

MR. PLESSER: Yahoo! is not an ISP.

MR. UNCAPHER: Yes, when Yahoo! is not an ISP, and why people get e-mail. If you -- for many people in America, where they get their e-mail is through their employer, where a T-1 or another line goes to the employer, where the "ISP" of that company is providing very limited service because the e-mail program is effectively hosted on the employer's site. So there really isn't a burden to put on that ISP. In effect, it's a burden that would be put on the employer to screen --

MR. PLESSER: I may be an old dog, and every time a certain bell rings I think of a certain approach, but maybe the way you have described it makes it look like more of a form, where the FTC would be in charge of enforcing the rules of the private network, and I think that's something that we have all had problems with over the years.

And I think that, you know, it's one thing to say that an ISP can have rules, and they should have rules, and they can manage their rules. It's an entirely different thing to say that the government -- that those rules essentially become governmental rules that the government enforces.

That's where I think, again, the industry has come together on saying that there shouldn't be a kind of governmental enforcement of ISP rules. Just like ISPs should

not become carriers, they should also -- the obverse should be true -- and their rules should not be like private law.

MR. RUBIN: And in fact, legislative history, I think, reflects that, in that some of the early drafts from the last Congress and earlier in this Congress explicitly allowed ISPs policies and procedures to be enforced by the rule of law. However, the legislation that passed explicitly says this shouldn't affect ISP's policies and procedures, one way or the other.

MR. SALSBURG: So Joe, from the Chamber of Commerce's perspective, if you have a member who is inundated with spam coming into their business domain, the business shouldn't have the right to say, "We don't want to get spam, we don't care that" --

MR. RUBIN: Well --

MR. SALSBURG: -- "that it's going to our employees that are using our e-mail accounts?"

MR. RUBIN: I mean, of course we support the ability -- and that's why we supported the CAN-SPAM Act. We think opt-outs can work.

But again, I mean, you get back to enforceability problems, and the consumer expectation problem. If -- you know, if a company wants -- one tool that we use, for example, that the Chamber uses is an e-mail filter system, which gives employees an opportunity to review the e-mail

later.

There are others like that that are available. Personally, I think it's a fantastic tool, and it really cuts down on my spam, and it makes it easy for me to sort through all that's left and say, "Well, this is legitimate, this isn't, this isn't."

But yes, of course we want the ability of companies to opt-out and to stop the flood of e-mail. But if you're only talking about 10 percent and some of that 10 percent could be, legitimate sales, that benefit both parties, for example, from a new supplier of widgets, who is trying to break into the market, could supply their e-mail address. If that e-mail gets filtered out as UCE, that doesn't benefit anybody, you know, if the company -- if that's --

MR. PLESSER: What I think your -- the domain wide registry says if under the registry model you propose domain owners, including ISPs, the supportive role in reading here is not only that the Chamber of Commerce could cut out that -- I mean, I think that's -- but you're also -- at least in the RFI -- suggesting that aol.com or yahoo.com, or any other .gov, you know, any other top-level domain --

MR. SALSBURG: Certainly we're not proposing these as being necessarily what the Commission is going to --

MR. PLESSER: We understand it's not -- we understand you ask a complete set of questions, but it does

say "including ISPs," so it triggers us to think of it at that level, as well.

But no, we understand that it's not an NPRM or a suggestion.

MR. CERASALE: One other thing. I think Joe mentioned one thing that I guess -- I will shift for a second, because otherwise I will forget about it.

Looking at one, two, and three -- four, as we talked about, it may not have this problem, but could also. One of the things that we worry about from a DMA standpoint -- and it's not really DMA members here, it's kind of DMA future members -- as we looked at the Internet as a low-barrier to entry in trying to get new entrepreneurs to come in and try and reach people, as we go to a "Do Not" -- go really to a "Do Not" system, presupposed prior to "Do Not" system with "Oh, you can get through if you opt-in," you eliminate from getting through to people the new company, the new entrepreneur. They can't get to you. They can't use the lower barrier to entry that the Internet provides. Or not even the Internet, but the e-mail provides.

The Internet, the search engines now become advertising vehicles where you get -- so even the web sites, there are so many of them, the Internet no longer is a way to try and -- for a new company to try and -- you have to try and drive traffic to your web site one way or another, and e-

mail allows that lower barrier entry.

You can't get it. You can't get that entrepreneur, job-creating engine that the Internet can be through e-mail. So I think all of this has a cost in the entrepreneurial side of the American economy -- a cost in the sense that we're losing a huge benefit that the Internet and e-mail provided.

MR. SALSBURG: Don't most anti-spam proposals have that same effect? Whitelists, for instance, the ability to --

MR. CERASALE: Well, it depends on -- the whitelist, if it says who you are, a whitelist -- that's why I didn't know on four. If it's who you are and I tell you to get on the whitelist, it depends on how you get on the whitelist. If to get on the whitelist you say, "Here is who I am, here is the ISP I'm coming from, here is where my address is, here is where you can find me," and that kind of thing, and I will put an opt-out in and honor it -- let's just add that one in there; I don't know if they have it.

Jerry Cerasale, in my garage -- I guess if I'm doing -- I can do that. Here is the address, here is the IP address it's going to come from, and so forth. I can meet that burden on the whitelist. If the whitelist requirement is, oh, a person has to know you and so forth, then right, the same thing I just said before would apply to that.

But if the whitelist is who are you, I know who you

are, I know I can get you, you promised to do this kind of stuff, and therefore we will put you on this List, we will take you off if you don't follow it, and maybe there will be other legal consequences, and so forth, that's why I say maybe it doesn't apply to four. The number four, you can work a whitelist situation out likely to get -- at least allow, at a low barrier to entry, you know, allow Jerry Cerasale Company to get in.

MR. SILVERSIN: How do you make the initial contact to get yourself on the whitelist?

MR. CERASALE: Well, there are companies that sell --

MR. SILVERSIN: Yes, you're telling me you're going to live by the rules and you're okay, but how do you approach me?

MR. CERASALE: How I approach you? Well, I would assume that if you're looking at the verified sender kind of thing, that there --

MR. SILVERSIN: You said domain wide, this is a domain wide list, rather than individual.

MR. SALSBURG: Yes. We're talking about ISP's whitelists --

(Several people speak simultaneously.)

MR. PLESSER: I mean but one of the things I think that we would think would be helpful in the report -- all

through your scenario -- but which I think we're starting to organize quickly to try to get to you is, you know, what the technologies are that are out there.

Yahoo! is itself coming out with what seems to be a great program. There are a lot of other programs that are developing, and I think that the market really needs to -- I think has gotten messages developed, and I think we think that it is.

And I think Jerry's point is to have government to come in and with this List would be to really stymie a lot of innovative solutions. And a mistake like allowing an ISP type opt-out because of public pressure, or whatever, will really change the dynamic.

MS. ROBBINS: Well, why don't we move on to the last model, and talk about that a little bit, since we --

MR. PLESSER: Time, what is your --

MS. ROBBINS: We're fine. It was from 1:00 to 3:00, so whenever we finish -- we could finish early, but you know --

MR. PLESSER: It would be embarrassing to finish early.

MR. SILVERSIN: I have a follow-up --

MR. PLESSER: Oh, good.

(Laughter.)

MS. ROBBINS: Any thoughts on that type of model?

MR. CERASALE: Yes, let's -- now, to verify, let me make sure I understand it first, before we get -- I can give a little bit and you can --

MS. ROBBINS: Okay.

MR. CERASALE: At some point there would be -- the verified sender would be -- I assume the government would oversee it to a certain extent, but I would deal with some central place where ISPs would go, and I would promise to do certain things. "Here I am, here is my IP address, this is what I do," and so forth. Is that the kind of thing you're looking at?

MS. ROBBINS: This proposal envisions a list maintained perhaps by the FTC.

MR. CERASALE: Okay.

MS. ROBBINS: So, you, as an e-mail marketer, would register your name, your domain names, and the IP addresses you're going to be sending mail from with the Federal Trade Commission. You would then receive a registration number. That registration number would have to go on your e-mails that you sent out.

MR. CERASALE: Sure.

MS. ROBBINS: So that way, when you send the e-mail and it goes to the ISP, the ISP then can say, "Here is a registration number." They can adjust their filters to say, "Okay, well here is the registration number, it matches the

IP address that it’s coming from --"

MR. CERASALE: Understand.

MS. ROBBINS: "-- and we will let it through."

MR. CERASALE: Okay.

MR. RUBIN: Is that a must-carry situation, or is -- is the ISP under any obligation to allow that --

MS. ROBBINS: They can adjust their filter to do whatever they want, yes.

MR. RUBIN: They could say there is no match.

MS. ROBBINS: Right.

MR. CERASALE: Or there is a match, and we're not going to let it through.

MR. RUBIN: Right.

MS. ROBBINS: Right.

MR. CERASALE: If their filters showed some other --

MS. ROBBINS: Right, right.

MR. CERASALE: Okay.

MR. SALSBURG: It's simply a method of authenticating that the sender is who the sender says it is.

MR. CERASALE: Right.

MS. ROBBINS: Right.

MR. CERASALE: Yes, that's similar to the kind of things that we have been trying to do and so forth with the -- I think that's --

(Several people speak simultaneously.)

MR. CERASALE: Yahoo! is working on that, as well as I think Gates has talked about the same kind of thing that Microsoft is working on. He's talked about also no persons -- it matches -- would there be any requirement -- you would -- I would register with the Trade Commission, and here is where -- here is my company, here is where I located, I assume, and here is what IP address I'm going to be sending from, and then I get a registration number and then I go.

And I guess we would still have to follow CAN-SPAM, because that's still the law of the land, and use it from that school. And then you would -- it's very much, in a sense, like a whitelist, except I guess everybody is eligible for it, including a spammer, but then you would know where they were.

MS. ROBBINS: Right.

MR. SALSBURG: The idea would be it would make the provisions of CAN-SPAM enforceable against the 90 percent who are using --

MS. ROBBINS: Right.

MR. CERASALE: And well, they wouldn't get through. They wouldn't be able -- we wouldn't have a -- I guess if they're worried about -- I don't know enough on security whether or not that tag is --

MR. PLESSER: Well, we do know that a large part of

the problem currently is where the spammers are throwing just all kinds of junk at the door, and that's flooding the systems. And a lot of that, a large percentage of that, doesn't even get through the front door. It stops at the initial filters.

MR. UNCAPHER: You would still have the spoofing problem.

MR. PLESSER: Well, A, you would have the spoofing problem, but you would also still have a -- could have -- two, you know, two million messages a day. Now you may have, you know, 100 million with registration numbers and then you would maybe -- you know, those would get through.

MS. ROBBINS: Could you explain how you think there would still be a spoofing problem?

MR. UNCAPHER: Well, we're assuming that as spammers currently impersonate -- spoof, legitimate senders, as a way of circumventing the filters that the ISPs put on, those exact same processes would -- the spammers would continue to use, and you just need to incorporate, to the extent they could, this authentication mechanism as a way of --

MS. ROBBINS: You mean being able to spoof the actual registration number?

PARTICIPANT: Both --

(Several people speak simultaneously.)

MS. ROBBINS: Right. Do you know if it's possible?

MR. PLESSER: But she's asking for a time out.

COURT REPORTER: One at a time, because --

PARTICIPANT: Okay.

MR. UNCAPHER: I guess it's hard. I mean, yes, theoretically the issue would be, can you have this authentication device be so bullet proof. It could certainly be if you can hijack a university's computer system to send out spam, then presumably technically it's going to be just as easy to be able to also impersonate an authenticated sender and send out the e-mail with that, that sort of certification that they were a legitimate sender --

MS. ROBBINS: Do you think it would make a difference if the registration number could be encrypted in the e-mail so that it's not visible? Do you think that would make a difference, technologically --

MR. UNCAPHER: Yes, that's where you kind of, at some point -- yes, that's theoretically possible. At some point, then, you run into this ISP issue, or this carriage issue. What are you requiring ISPs to do, and what are you requiring ISPs to do in terms of filtering?

We talked about the issue of employers and there are obviously -- there are 1,500 ISPs, but the managers of mail accounts are far more than that. What kind of burdens -- what are you expecting them to do? I mean, basically, who

are you expecting to have the capacity, technically, to be able to use this mechanism?

You know, if you put the burden on the employer, then you will run into this issue of, frankly, you have got such a large population potentially having the key to this encryption as to render it useless.

So, it's possible to create it, but you end up with a lot of these difficult problems.

MR. RUBIN: The other side is the -- I think extreme -- danger perhaps of being overly broad in that, you know, going back to Ron's earlier point, the definition of UCE, you know. When do you have to get this authentication, when do you not have to -- the transactional, and what do you do about companies that are sending non-commercial e-mails? You know, if they're sending out their newsletter, for example, or a charity sending out non-commercial solicitation, or something along those lines.

Or, even just personal e-mail back and forth, you know, you're making it -- I think, raising the stakes and making it more likely that an ISP is going to block legitimate e-mail, just set their filters extremely high so that only stuff with this -- with the tag comes through, and then you block, you know, all the other legitimate --

MR. PLESSER: Well, the other -- the axiom to that is that everybody would have to register. Then if I want to

send an e-mail to my kid in Clinton, New York, I would have to register. The e-mail systems can't differentiate between me sending an e-mail to my son or somebody sending out a million. I mean, they can distinguish volumes, but they can't distinguish the content of it.

So, if you need a registration number to get through the system, then everybody is going to need a registration number to get into the system. And then I think, you know, then you will hear from the ACLU and from a lot of other people in terms of having -- you know, law enforcement guys might like that, but then you're really requiring registration of all e-mail to get through.

At least that's the danger of how it could be interpreted. I know that's not your intent, but I think that that's -- and again --

MR. SALSBURG: So if a model were set up to only be triggered by the sending of over X number of e-mails, would that be a solution to this problem?

MR. PLESSER: Well, probably not, because they duck behind limits.

PARTICIPANT: Tell them what the threshold is, and they will drop it by one.

MR. PLESSER: They will drop it by one.

MR. SALSBURG: But every time you drop the threshold, you're increasing their costs, because they have

to find one more compromised proxy.

MR. UNCAPHER: Although, obviously, they send out packets, if you -- I mean, they could get around that, as well.

MR. SALSBURG: Does anyone know how the private authentication plans -- Yahoo!'s, AOL's, and Microsoft's -- are dealing with the issue of the small sender?

MR. UNCAPHER: Well, there are a variety -- I mean, Joe mentioned one. I have one if my list is triggered by, if I send an e-mail to somebody -- so Jerry sends me something and I send him back, a list that's been authenticated for me, I mean, that's just one particular -- there are obviously other mechanisms that work.

I mean, and I think to go back to a point that Ron made, that this is an area where there is a lot of -- since there is clearly a demand for it, there has been a lot of development as to kind of what the best process is. We try a new filter every week now, to see what the best mechanism is.

MR. CERASALE: I don't know -- we only know from the press what Yahoo! and Microsoft are looking at. I know they're looking at connecting the IP address with the -- I don't know how exactly they're going to do that. Are they going to know that this IP address is from Ford Motor Company, and then look in to see if Ford is an e-mail message or whether -- I don't know.

I mean, that would be something to -- that is beyond my expertise, and it's probably a decent question as you look at item number four here, to see what they're doing on that authentication, what they're thinking about.

MR. RUBIN: I think this whole discussion underlies the marketplace solution, in that different ISPs and different companies are experimenting with different solutions, AOL's trying what they're trying, and you know, there are various companies offering various filter systems.

But -- and what we're seeing is competition in trying to get rid of the spam. And so, you know, ISPs are trying different mechanisms and trying to see what works and what works better, trying to keep one step ahead of the 90 percent.

And one of the concerns, I think, with an authenticated sender is it might sort of stifle the innovation a little bit, might say, "Well, you know, you don't need to spend millions of dollars a year trying to stop spam, we can just turn up our filters and let the legitimate commercial e-mail through, and if we end up blocking some legitimate non-commercial e-mail, then that's too bad, but at least it's saving us millions of dollars."

MR. PLESSER: One of the issues that I think cuts across all -- certainly the first three -- that we probably didn't talk about, was authentication of how do you get on

the list.

And you know, we have found with the Do Not Call Registry, I think it's different, perhaps, with the fact that -- because the agencies have so much information, they can probably do an authentication that's pretty accurate. But in the Do Not Call Registry we have found that the sign-ups have not been very good.

Somebody put Jerry's number on the Do Not Call Registry during the crisis month of October/November, and it took him a day or two to get it off, because it's harder to get things off than to get them on to that system.

But I think the authentication issue is very important, in terms of making sure it really is -- that people who are opting out really are persons associated with that e-mail, and we have experience that that does not work very well --

(Several people speak simultaneously.)

MR. SALSBURG: Is there a sense of whether or not it's more than an aberration? I mean, is this --

MR. CERASALE: A Do Not Call? I do not necessarily --

MR. PLESSER: Well, we do in a certain perspective. I mean, I think the average sign-ons are larger than certainly the telephone sign-ons, and people are doing multiples. Whether or not there are multiple telephone

numbers -- they are doing it for their relatives, or they are doing it out of irony and spite, like the one person who did it to Jerry, I don't know.

But we know there are significant kind of additional -- that the List is far greater than I think the people really intended to -- maybe that's because they put three numbers down, you know, home number, cell number, vacation home number, so somebody may put four numbers down.

But I think there is some indication that proves it's been pretty significant, particularly because of the authentication problems.

MR. SALSBURG: Could there be ways to solve this problem, such as using double opt-out?

PARTICIPANT: Yes, I think there are ways to resolve --

MR. PLESSER: Yes, there are -- and I think, for example, the fact that registration for a free credit report won't be as bad as a Do Not Call Registry, because there are technologies available because of the amount of data -- if you're requesting your own credit report, and they have the credit report, there is a lot of data that can be matched to make sure that it's the right person. That's not true in some of these other registry programs.

MR. CERASALE: Yes. On the Do Not Call and the Internet you put in a number and you add an e-mail address,

and then the response went to the e-mail address, and then you had a response back.

(Several people speak simultaneously.)

MR. CERASALE: Yes, the e-mail address would be what is going on, whereas there is no connection between the phone number and the e-mail address in the Do Not Call -- so you know, it's better that way, and you know, we know there are fax numbers and stuff on that List which shouldn't be there, and so forth.

I do have to set one piece of the record straight, since this is potentially -- the reason it took me a couple of days to get off the list was, in large part, due to the fact that DMA won a lawsuit initially, and the FTC had to pull the list down. So it took a little bit of time to -- put it back up.

(Several people speak simultaneously.)

MR. CERASALE: That was done so I could get the name off.

PARTICIPANT: That's right.

MR. PLESSER: Really, it was because you couldn't go home, because --

(Several people speak simultaneously.)

MR. PLESSER: What other -- what information -- not just today, but we're happy to, you know, on the record -- would be helpful for people at this table or other meetings

to present to you? What kind of information or facts would be helpful to -- that you would find in this report that you have to get out in an extraordinary period of time?

MR. SALSBURG: Well, one thing that you mentioned -- I think it was Mark, you mentioned the churn rate for e-mail accounts.

MS. ROBBINS: Yes.

MR. SALSBURG: Could you actually show that the churn rate is much higher than telephones? I think that would be interesting. One of the practical considerations we have to look at is database management.

MS. ROBBINS: Right.

MR. SALSBURG: And that's a very valid issue.

MR. UNCAPHER: Anecdotally -- Jerry probably has the same problem -- I mean, my association membership base knows how representative it is, but judging from the e-mail that we send out that we then get bounce-backs from -- these are members who signed up -- your 6-month is probably a pretty good number, because it does seem that every month or so you lose about 5 or 10 percent.

Now, they may just be people with new e-mail addresses within their own organizations. But as for a general number, I could probably try and find that out.

MR. CERASALE: Yes, we will send some word out and see what kind of information we can get, and we will supply

that to you. Not certain --

MR. SALSBURG: I don't know if the data is out there, but I mean, if --

MR. CERASALE: We will try our best to tell you what we got and how we got it.

PARTICIPANT: Yes.

MS. ROBBINS: Does anyone else have any other thoughts on any of these models before we wrap up?

MR. PLESSER: I have a feeling we have a lot, but I don't know that we -- I think we intend to probably send some things in and write some things.

I think we can -- we understand your response on the privacy threat issue, and I think, you know, we still think it's very significant, and will document it.

Obviously, some of these alternatives -- the second one or the third one, the e-mail forwarding is an intent to resolve that, although I still think that there are problems, you know, that there have been problems with thefts and stuff with third parties. The FTC itself has investigations undergoing, I think, on some of those kinds of issues.

And I think we just have to look at the balance between cost to the FTC to enforce, cost for industry against the interest of the consumer. And I think the CAN-SPAM Act technological developments are things that are going to work.

And you know, maybe one of the solutions here is to

have the question of a list put off for a while. You know, let's see how the current mix is working before you do something that's Draconian.

We will, I think, come in with some material to indicate that we think -- that we would think that an e-mail list will have a significant impact on legitimate -- on the 10 percent. And I think the advocates who want to get the 10 percent, you know, I really don't understand that.

I mean, I don't understand why they want to get the 10 percent, assuming that the definitions of UCE and current operations -- the complaints that we hear do not come about -- from the 10 percent, they come from the 90 percent.

MR. RUBIN: Is there just an assumption that the 90 percent bad guys you're not going to touch at all? Is that -- I mean --

MR. SALSBURG: No, there are no assumptions.

MS. ROBBINS: No.

MR. RUBIN: Okay. I mean, it sounds like the List is aimed pretty squarely at the 10 percent who already follow the law. And at least from our perspective, and other folks here, we think that most of the focus should be on the bad guys.

And you know, obviously, we would like to see the FTC focus your resources on stopping the bad guys.

And we think, again, you have a unique role to

play, and a very strong role to play, and that you really could, working with the State Attorneys General and the Justice Department, and through technological means, and through -- with the ISPs and others, really could make a dent in that 90 percent. And that's where, you know, we hope that you would focus most of your effort.

MR. CERASALE: But we do know that you're doing this because someone told you. This is not --

MR. PLESSER: Lou, did you have some questions?

MR. SILVERSIN: Yes, I had some questions, but I don't know if these guys want to stick around for that. Other enforcement issues, you know.

MS. ROBBINS: Thank you for taking the time.

MR. SALSBURG: Thank you.

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P044405

CASE TITLE: DO NOT E-MAIL REGISTRY MEETING

DATE: MARCH 9, 2004

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the tapes transcribed by me on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MARCH 15, 2004

LISA SIRARD

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE